REMARKS

Claims 1-32 are pending in this application.

Claims 1, 9, 17, 18, and 26 are independent.

The drawings are objected to. Corrected drawings are submitted herewith. Approval is courteously requested.

Claim 14 is objected to because of a minor editorial error. Accordingly, claim 14 is amended to correct this minor editorial error and for no other purpose.

Claims 17 and 26 stand rejected under 35 USC §102(b) as being anticipated by Ganesan (U.S. Patent No. 5,535,276). Claims 1-16, 18-25, and 27-31 stand rejected under 35 USC §103(a) as being obvious over Ganesan in view of Spies (U.S. Patent No. 6,230,269). The rejections are respectfully traversed.

Claims 17 and 26 require, inter alia, generation of a first private key portion of a private crypto-key associated with a user, the user's crypto-key having the first private key portion and a second private key portion; transformation of a first message with the generated first private key portion; and a further transformation of the first message with the second private key portion. Also required by claims 17 and 26, the first private key portion is not stored at any networked device and is not transmitted over a network.

The Examiner looks to Ganesan at column 8, lines 24-32, column 14, lines 59-66, and column 15, lines 52-54 and 61-63, in rejecting these claims. In particular, the Examiner argues that Ganesan discloses "a first networked device ... that generates a first private key portion, transforms a message with the first portion to form a second message ... and transmits the second message. .... Ganesan also discloses a second network device that stores a public key and a second private key portion..., receives the

second message, and further transforms the second message with the second private portion."

It is respectfully submitted that the Examiner's reading of Ganesan is mistaken. In Ganesan, a user is associated with an asymmetric crypto-key having a public key portion and a private key portion. For the sake of discussion herein, this asymmetric crypto-key will be referred to as the permanent key. The private key portion of the permanent key is divided into a first portion, known only to the user, and a second portion which is stored on a database (see, for example, column 15, lines 19-26).

The user generates a temporary asymmetric crypto-key having a temporary private key portion and an associated temporary public key portion. The generated temporary public key portion is then encrypted with the first private key portion of the permanent key to form a first message (see, for example, column 8, lines 20-28). The first message is transmitted to a security or authentication server or processor which applies to the first message the second private key portion of the permanent key and the public key portion of the permanent key to obtain the temporary public key. The server or processor then further encrypts the first message with the second private key portion of the permanent key to form a second message (see, for example, column 8, lines 29-37).

Thus, Ganesan does not disclose transformation of a message with a user generated first key portion, as argued by the Examiner. Rather, Ganesan discloses two separate crypto-keys associated with a user: the permanent key and the temporary key that is generated by the user. A public portion of the user-generated temporary key is

encrypted with a private portion of the permanent key, not any portion of the generated temporary key, or any portion of any key generated by the user.

Furthermore, as best understood, the Examiner has completely ignored expressly recited claim limitations of claims 17 and 26. For example, the Examiner never addresses the requirements that the first private portion of the private crypto-key not be stored at any networked device and not transmitted over a network. Accordingly, the Examiner has failed to meet the burden in establishing a prima facie case for the rejection.

In view of the deficiencies in Ganesan and the failure to consider certain claim limitations, it is respectfully requested that the Examiner reconsider and withdraw the rejection of claims 17 and 26, as well as the rejection of claims 27-31, which depend from claim 26.

Independent claim 1 requires, inter alia, a first processor configured to generate a private crypto-key and a corresponding public crypto-key, divide the private crypto-key into a first private key portion, based on a password of a user, and a second private key portion, destroy the private crypto-key and the first private key portion without distribution thereof and without storage thereof in a persistent states, and store only the second private key portion and the public crypto-key in a persistent state. Also required by claim 1 is a second processor, representing a user, configured to generate only the first private key portion responsive to receipt of an inputting of and based on the user password, and destroy, without storing in a persistent state, the generated first private key portion.

The Examiner argues that Ganesan discloses the recited first processor and second processor. However, the Examiner's position is not understood because the Examiner points to the same processor (at column 14, lines 29-32) as being both the first processor and the second processor. The claim expressly requires a first processor and a second processor, but the Examiner only points to a single processor in rejecting the claim.

Also, the Examiner argues, pointing to column 14, line 66, through column 15, line 2, and column 19, lines 27-29, that Ganesan discloses a first processor destroying a generated private key and first private key portion, and a second processor destroying a generated first private key portion. Again, the Examiner relies upon disclosure of a single processor, not two processors. Ganesan simply does not disclose two processors, each configured as recited in claim 1. This is even highlighted in the Examiner-referenced text bridging columns 14 and 15: "key generation information has been destroyed, preferably within the safe confines of the tamper proof chip used to generate the crypto-keys." Thus, a single chip generates and destroys keys in Ganesan.

Further, the Examiner's arguments regarding destruction are at best speculative, as all that is disclosed regarding destruction is that a first private portion is known only to a user, a second private portion is stored on a secure database, and "all other intermediate key generation information has been destroyed." Ganesan does not teach or suggest a first processor generating a private crypto-key and destroying the generated private crypto-key and a first private key portion of the generated private

crypto-key, and a second processor, representing a user, generating only the first private key portion and destroying the generated first private key portion.

Also, the Examiner has seemingly ignored the express requirements that the first processor not store in a persistent state or distribute the private crypto-key, and that the second processor not store the first private key portion in a persistent state. Thus, as with claims 17 and 26, for this reason alone the Examiner has failed to establish a prima facie case for the rejection.

The Examiner acknowledges that Ganesan does not teach or suggest that the first processor divides the private crypto-key based on a password of the user, and that Ganesan does not teach or suggest that the second processor generates the first private key portion responsive to receipt of an inputting of, and based on, the user password. The Examiner looks to Spies to cure this defect. While Spies does generally disclose the use of passwords in generating keys, Spies does not teach or suggest that required by claim 1. In particular, Spies does not teach or suggest division of a private key based on a password, or generation of only a first portion of a private key responsive to receipt of an inputting of, and based upon, the user password. Rather, in Spies, an entire public-private key pair is generated based at least in part upon a password. In any event, it is respectfully submitted, even if Spies disclosed what the Examiner seems to contend (which it is respectfully submitted Spies does not), a combination of Ganesan and Spies would not cure the defects of the Ganesan reference discussed above.

Accordingly, in view of the above, it is respectfully requested that the Examiner reconsider and withdraw the rejection of claim 1, as well as claims 2-8 which depend from claim 1.

Regarding independent claim 18, this claim requires, inter alia, generation, based upon a password of a user, a private crypto-key and a corresponding public crypto-key associated with the user, division of the private crypto-key into a first private key portion and a second private key portion, destruction of the private crypto-key and the first private key portion without distribution thereof and without storage thereof in a persistent state, separate generation, responsive to receipt of, and based upon, the user password, of only the first private key portion, and destruction, without storage in a persistent state, the separately generated first private key portion.

The Examiner relies upon the same grounds to reject claim 18 as relied upon in rejecting claim 1. Similar to claim 1, claim 18 requires a first generation of a private crypto-key having first and second private portions and a corresponding public crypto-key, and a separate generation of only the first private portion. The Examiner looks to disclosure of a single generation (at column 14, lines 29-32) of a public/private key pair in which the private key has multiple portions. Ganesan in no way teaches or suggests a separate generation of only the first private portion, as required by claim 18.

The Examiner acknowledges that Ganesan does not teach or suggest that the private crypto-key and the first portion are generated based on the user's password. The Examiner looks to Spies to cure this defect. While Spies does generally disclose the use of passwords in generating keys, Spies does not teach or suggest a separate generation of only the first private key portion based upon a password. Additionally, a

combination of Ganesan and Spies does not cure the other defects of Ganesan discussed above.

Also, the Examiner has seemingly ignored the express limitation that the private crypto-key and first private key portion be destroyed without distribution thereof, as well as the express limitation that the separate generation take place responsive to receipt of the user's password. This alone results in the Examiner failing to make a prima facie case for the rejection.

In view of the above, it is respectfully requested that the Examiner reconsider and withdraw the rejection of claim 18, as well as claims 19-25, which depend from claim 18.

Claim 9 requires, inter alia, a first processor, representing a user, configured to generate a first potion of a private crypto-key based upon a user password, transform a message with the first private key portion, and destroy the generated private key portion after transforming the message. Also required by claim 9 is a second processor configured to further transform the transformed message by applying at least one of a second portion of the private crypto-key and a public crypto-key, both of which correspond to the first private key portion.

As discussed above, Ganesan discloses a permanent key associated with a user having a public key portion and a private key portion, the private key portion having a first portion and a second portion, and a temporary user-generated key having a public portion and a private portion. The user generated temporary public key portion is encrypted with the first private key portion of the permanent key to form a first message. The first message is transmitted to a security or authentication server or processor

the first private key portion has a bit length of at least 257 bits. The Examiner's argument regarding these claims consists of "the user password has a bit length between 56 and 72 bits." Thus, the Examiner seems to have ignored the express limitation that the private key portion have a bit length of at least 257 bits. Further, the disclosure upon which the Examiner relies merely recites that 64 bit passwords are undesirable (column 3, lines 31-40), and that a first private key portion be "short in length, e.g. 8 to 12 characters."

Claims 4, 13, 21, and 29 require, inter alia, selectively operating in one of two modes such that if operating in the first mode, a one way function is applied to the password a first number of times to generate the first private key portion, and if operating in the second mode, the one way function is applied to the password a second number of times, different than the first number of times, to generate the first private key portion. The Examiner looks to Spies in rejecting these claims. However, Spies simply does not disclose selectively operating in one of two modes. The Examiner-referenced text merely discloses multiple implementations. No where does Spies even suggest that the multiple implementations can somehow be combined to form a technique of selective operation. At most, Spies discloses that a processor "computes one or more one-way hash functions of the user ID and password P." Spies in no way discloses a first number of hash functions and a second number of hash functions selectively applied.

Claims 5, 7, 14, 16, 22, 23, 30, and 31 require, inter alia, a selection of a one way function or mode of operation based upon at least one of an identity of the user and a strength of the user password. The Examiner's rejection consists of "Spies further

which applies to the first message the second private key portion and the public key portion of the permanent key to obtain the temporary public key.

Ganesan does not disclose a user processor generating a first portion of a private crypto-key and then transforming a message with that generated first portion of the private crypto-key. Rather, Ganesan discloses generation of a temporary key, and encryption of that generated key with a portion of the permanent key. Also, contrary to the Examiner's position, Ganesan does not disclose a user processor destroying a generated private key portion after transformation of a message with that portion. At most, Ganesan generally discloses that information used to create a key is destroyed.

The Examiner acknowledges that Ganesan does not teach or suggest that the first private portion is generated based on the user's password. Again, the user looks to Spies to cure this deficiency. As discussed above, while Spies does generally disclose the use of a password in generating a key, Spies does not disclose a user processor generating a first portion of a private crypto-key based on a user password. Furthermore, even if Spies did disclose that claimed (which it is respectfully submitted Spies does not) a combination of Ganesan and Spies would not cure the defects of Ganesan discussed above.

Accordingly, in view of the above, it is respectfully requested that the Examiner reconsider and withdraw the rejection of claim 9, as well as claims 10-16, which depend from claim 9.

The dependent claims of the present application also recite features that are neither taught nor suggested by the applied art. For example, claims 2, 11, 19 and 27 require, inter alia, that the user password has a bit length of between 56 and 72 bits and

discloses relying on the strength of the user password in generating keys (column 8, lines 19-21). The Examiner's position is not understood, as the relied-upon text teaches "In another less preferred implementation, the client can be configured to generate a public/private key pair as a function of only the user password and user ID. In theory, if passwords are well chosen, the authentication system can use entropy in the password to generate the user private key." Thus, the relied upon text fails to teach or suggest any selection, fails to teach or suggest a selection of a one way function or mode of operation, and fails to teach or suggest a selection based upon a user identity or a strength of a user password.

Claims 6 and 15 require, inter alia, a selection of a one way function from a group of one way functions. The Examiner relies upon column 5, lines 42-46, of Spies in rejecting these claims. The relied-upon text discloses a first and a second one-way hash function. However, no selection between those functions is disclosed.

Claims 8 requires, inter alia, that the second processor be further configured to encrypt or sign a message with the first private key portion prior to destroying the generated first private key portion. Claim 24 requires, inter alia, transforming a message with the generated first private key portion prior to destruction thereof. As discussed above, Ganesan does not disclose generating a first private key portion and encrypting a message with that generated portion. Rather, Ganesan discloses an temporary entire public/private key pair, and encrypting the generated temporary public key with a first private portion of the permanent private key.

Claims 10 and 25 require, inter alia, that the first private key portion never be stored in a persistent state. The Examiner looks to column 14, line 59, through column

15, line 2, in rejecting these claims. The relied-upon text merely teaches destruction of intermediate key generation information. That the first private key portion never be stored in a persistent state is not taught by Ganesan or Spies.

Thus, the dependent claims of the present application are patentably distinguishable from the applied art over and beyond the distinctions found in the independent claims. Accordingly, at least for the reasons above, it is respectfully requested that the Examiner reconsider and withdraw the rejection of the dependent claims of the present application.

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed local telephone number, in order to expedite resolution of any remaining issues and further to expedite passage of the application to issue, if any further comments, questions or suggestions arise in connection with the application.

To the extent necessary, a petition for Extension of Time is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including any extension of time fees, to the Deposit Account No. 01-2135 (Case No. 1160.41369X00) and please credit any excess fees to such Deposit Account.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Sterling W. Chandler
Registration No. 51,370

1300 North Seventeenth Street
Suite 1800
Arlington, VA 22209
Tel.: 703-312-6600
Fax.: 703-312-6666

SWC